NSS 123

(INTRODUCTION TO NETWORKING DEVICE)

WHAT ARE NETWORK DEVICES?

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

TYPES OF NETWORK DEVICES

Here is the common network device list:

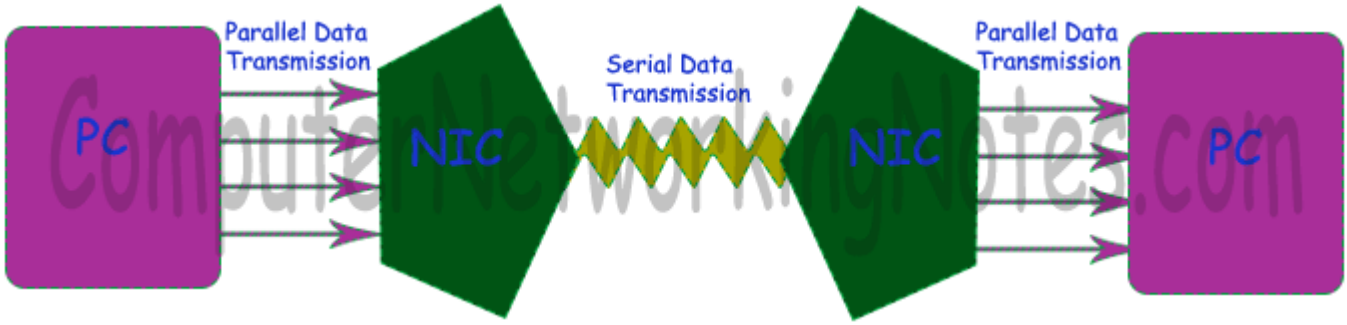
- NIC
- Hub
- Switch
- Router
- Bridge
- Gateway
- Modem
- Repeater

1. NETWORK INTERFACE CARD (NIC)

In the list of the networking devices, NIC stands on the first place. Without this device, networking cannot be done. This is also known as network adapter card, Ethernet Card and LAN card. NIC allows a networking device to communicate with the other networking device.

NIC converts the data packets between two different data transmission technologies. A PC uses parallel data transmission technology to transmit the data between its internal parts while the media that provides connectivity between different PCs uses serial data transmission technology.

A NIC converts parallel data stream into the serial data stream and the serial data stream into the parallel data stream.



Typically all modern PCs have the integrated NICs in the motherboards. If additional NICs are required, they are also available as add-on devices separately.

For desktop or server system, they are available in the adapter form which can be plugged into the available slots of the motherboard. For laptop or other small size devices, they are available in the PCMCIA (Personal Computer Memory Card International Association) card form which can be inserted into the PCMCIA slot.

TYPES OF NICS

There are two types of NICs.

MEDIA SPECIFIC: - LAN card are used according to the media type. Different types of the NICs are used to connect the different types of media. To connect a specific media type, we must have to use a NIC which is particularly made for that type of media.

NETWORK DESIGN SPECIFIC: - A specific network design needs a specific LAN card. For example FDDI, Token Ring and Ethernet have their own distinctive type of NIC cards. They cannot use other types of NIC cards.

Following figure illustrates some common types of NICs.

2. **HUB**

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model

HUB

TYPES OF HUB

ACTIVE HUB: - These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

PASSIVE HUB: - These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

FEATURES OF HUB

Here are important features of Hub:

- It works with broadcasting and shared bandwidth.
- It has 1 broadcast domain and 1 collision domain
- Works at the physical layer of the OSI model
- A virtual LAN can't be created using a hub
- Provides support for half-duplex transmission mode
- A hub has just a single broadcast domain
- Does not support spanning tree protocol
- Packet collisions occur mostly inside a hub

APPLICATION OF HUBS

The important applications of networking hub are given below:

- Hubs are used in organizations for connectivity.
- They are used for creating small home networks.
- It is used for network monitoring.
- You can create a device or peripheral which is available thought out the network.

ADVANTAGES OF HUB

- Offers shared Internet Scalability (uplink)
- Allows Network Monitoring
- Provide backward compatibility
- Helps you to extend the total distance of the network

DISADVANTAGES OF HUB

- It's mostly half-Duplex
- Does not offer dedicated bandwidth
- It cannot select Network's Best Path.
- There is no mechanism of any kind to reduce network traffic.
- Possibility of the device differentiation
- Network size

3. SWITCH

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer or the Network layer of the OSI model. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

SWITCH

TYPE OF SWITCH

MANAGEABLE SWITCHES: Manageable switch has a console port and IP address, which can be assigned and configured.

UNMANAGEABLE SWITCHES: On an Unmanageable switch, configuration can't be made. It is not possible to assign IP address as there is no console port.

FEATURES OF SWITCH

Here are important features of switch:

- It is Datalink layer device (Layer 2)
- It works with fixed bandwidth
- It maintains a MAC address table
- Allows you to create virtual LAN
- It works as a multi-port bridge
- Mostly comes with 24 to 48 ports
- Supports half and full-duplex transmission modes

APPLICATIONS OF SWITCHES

Some applications of switches are:

- A switch helps you to manage the flow of data across the network.
- Medium to large-sized LANs containing a number of linked managed switches.
- Switches are widely used in SOHO(Small Office/Home Office) applications. SOHO mostly uses a single switch to access the various broadband services.
- It is used in a computer network to connect the devices together physically.
- A switch can transfer data to any of the other devices, either using half-duplex mode or full-duplex mode.

ADVANTAGES OF SWITCH

Here are pros/benefits of using Switch

- ✓ It helps you to reduce the number of broadcast domains.
- ✓ Supports VLAN's that can help in Logical segmentation of ports
- ✓ Switches can make use of CAM table for Port to MAC mapping

DIFFERENCE BETWEEN SWITCH AND HUB

Hub	Switch
A hub operates on the physical layer.	A switch operates on the data link layer.
Hubs perform frame flooding that can be unicast, multicast, or broadcast.	It performs broadcast, then the unicast and multicast as needed.
Just a singular domain of collision is present in a hub.	Varied ports have separate collision domains.
Transmission mode is Half-duplex	Transmission mode is Full duplex
A hub operates as a Layer 1 devices per the OSI model.	Network switches help you to operate at Layer 2 of the OSI model.
To connect a network of personal computers should be joined through a central hub.	Allow connecting multiple devices and ports.
Uses electrical signal orbits	Uses frame & packet
Does not offer Spanning-Tree	Multiple Spanning-Tree is possible
Collisions occur mostly in setups using hubs.	No collisions occur in a full-duplex switch.
Hub is a passive device	A switch is an active device
A network hub can't store MAC addresses.	Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips).
Not an intelligent device	Intelligent device
Its speed is up to 10 Mbps	10/100 Mbps, 1 Gbps, 10 Gbps

Does not use software	Has software for administration

4. **REPEATER**

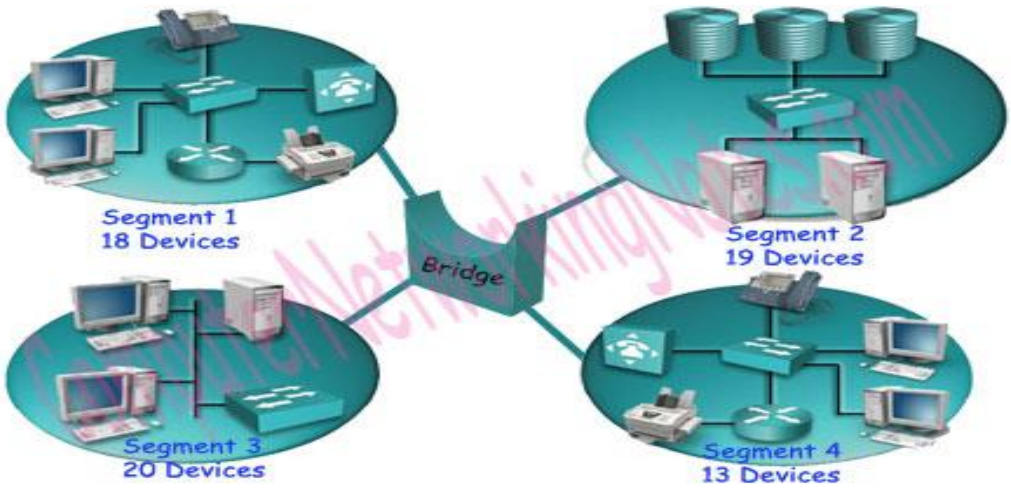
A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

5. **BRIDGE**

A bridge is a repeater; with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Bridge is used to divide a large network into smaller segments. Basic functions of the Bridge are the following: -

- Breaking a large network into smaller segments.
- Connecting different media types. Such as connects UTP with the fiber optic.
- Connecting different network architectures. Such as connects Ethernet with the Token ring.



A Bridge can connect two different types of media or network architecture, but it cannot connect two different types of network layer protocol such as TCP/IP or IPX. Bridge requires the same network layer protocol in all segments.

THERE ARE THREE TYPES OF BRIDGE:

LOCAL BRIDGE: - This Bridge connects two LAN segments directly. In Ethernet Implementation, it is known as the Transparent Bridge. In Token Ring network, it is called the Source-Routed Bridg

REMOTE BRIDGE: - This Bridge connects with another Bridge over the WAN link.

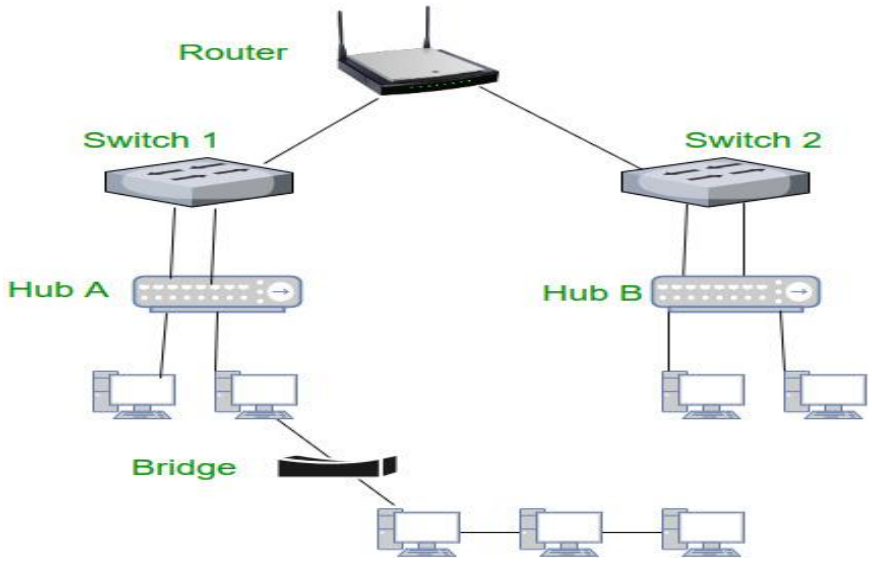
WIRELESS BRIDGE: - This Bridge connects with another Bridge without using wires. It uses radio signals for the connectivity.

In OSI Layers /TCP-IP networking models, the functionalities of the Bridges are defined in the physical layer and data link layer.

Just like Hubs, Bridge no longer used in the computer network. Bridges have been replaced by the Switches.

6. **ROUTERS**

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



ADVANTAGES OF ROUTER OVER OTHER NETWORKING DEVICES

BENEFITS OR ADVANTAGES OF ROUTERS

Following are the benefits or advantages of Routers:

➡It provides connection between different network architectures such as ethernet & token ring etc.

➡It can choose best path across the internetwork using dynamic routing algorithms.

➡It can reduce network traffic by creating collision domains and also by creating broadcast domains.

➡It provides sophisticated routing, flow control and traffic isolation.

➡They are configurable which allows network manager to make policy based on routing decisions.

DRAWBACKS OR DISADVANTAGES OF ROUTERS

Following are the drawbacks or disadvantages of Routers:

➡They operate based on routable network protocols.

➡They are expensive compare to other network devices.

➡Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.

➡They are slower as they need to analyze data from layer-1 through layer-3.

➡They require considerable amount of initial configurations.

➡They are protocol dependent devices which must understand the protocol they are forwarding.

DIFFERENCES BETWEEN ROUTER AND SWITCHES

POINTS OF DIFFERENCE	ROUTERS	SWITCHES
Mode of transmission of data	It Transmits data in the form of packets.	It Transmits data in the form of frames.
Address used for the purpose of data transmission.	It makes use of IP address for the purpose of data transmission.	It makes use of MAC address for the purpose of data transmission.
Layer of OSI Model	It makes use of layer 3 of OSI model. Layer 3 is the network layer.	It makes use of layer 2 of OSI model. Layer 2 is the Data Link Layer.
Ports	Routers contain 2 Ports by default like fast Ethernet Ports. However, we can add serial ports explicitly.	Switches, on the contrary, are available with different Ports i.e – 8, 16, 24, 48 and 64.
Table	It makes use of the Routing Table for routes to get to the destination IP.	It makes use of CAM (Content addressable Memory) table for MAC address.
Broadcast domain	Routers break the broadcast domain and it does not propagate broadcast domain.	Switches allow the broadcast domain and contain per port collision domain.
Function	Router in networking is used to connect two different Networks	It is used to connect End devices such as computers, printers, scanners etc.
Used for	It is used for both WAN/LAN networks.	It is only used for the LAN networks.

Mode of Transmission	By default, Router is in full duplex mode. However, we can change them manually into half-duplex.	Switches are used in half as well as full duplex mode. However, we can also make them in auto-negotiation.
NAT (Network Address Translation) and PAT (Port Address Translation).	In Routers, we can perform Network Address Translation as well as Port Address Translation	In Switches, we can neither perform Network Address Translation nor Port Address Translation.

7. **GATEWAY**

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. Gateways normally work at the Transport and Session layers of the OSI model, Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and are generally more complex than switch or router.

EXAMPLES OF THE GATEWAY

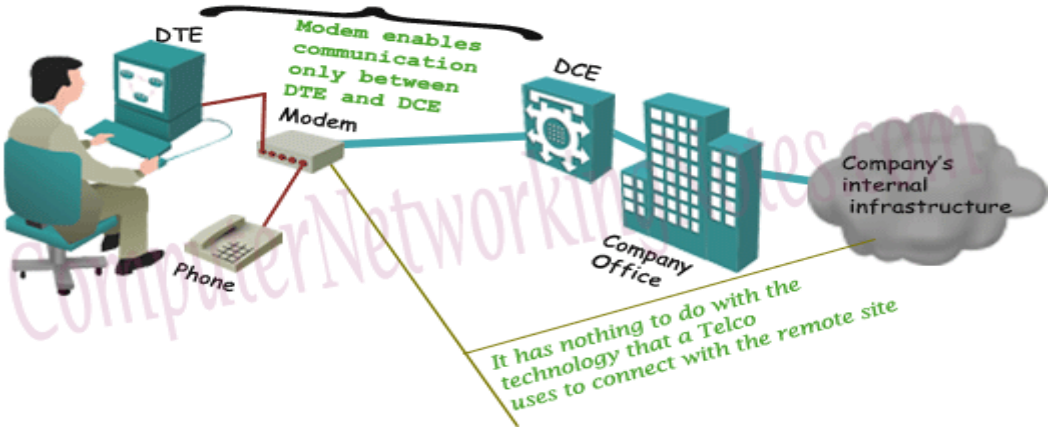
EMAIL GATEWAY: - Translates SMTP e-mail in standard X.400 format before forwarding.

GSNW GATEWAY: - Allows Windows clients to access resources from the NetWare server.

PAD GATEWAY: - Provides connectivity between LAN network and X.25 network.

8. MODEM

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232. Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.



WHAT IS OSI MODEL?

The International Standards Organization (ISO) developed the Open Systems Interconnect (OSI) model in 1981. It consists of seven functional layers that provide the basis for communication among computers over networks, as described in the table below. You can easily remember them using the mnemonic phrase "All people seem to need data processing." Understanding this model will help you build a strong network, troubleshoot problems, develop effective applications and evaluate third-party products.

LAYER	FUNCTION	PROTOCOLS OR STANDARDS
Layer 7: Application	Provides services such as e-mail, file transfers and file servers	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, RLogin, BootP, MIME
Layer 6: Presentation	Provides encryption, code conversion and data formatting	MPEG, JPEG, TIFF
Layer 5: Session	Negotiates and establishes a connection with another computer	SQL, X- Window, ASP, DNA, SCP, NFS, RPC
Layer 4: Transport	Supports end-to-end delivery of data	TCP, UDP, SPX

LAYER	FUNCTION	PROTOCOLS OR STANDARDS
Layer 3: Network	Performs packet routing	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2: Data link	Provides error checking and transfer of message frames	Ethernet, Token Ring, 802.11
Layer 1: Physical	Physically interfaces with transmission medium and sends data over the network	EIA RS-232, EIA RS-449, IEEE, 802

CHARACTERISTICS OF OSI MODEL

Here are some important characteristics of the OSI model:

- A layer should only be created where the definite levels of abstraction are needed.
- The function of each layer should be selected as per the internationally standardized protocols.
- The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.
- In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer.
- Changes made in one layer should not need changes in other lavers.

WHY OF OSI MODEL?

- Helps you to understand communication over a network
- Troubleshooting is easier by separating functions into different network layers.
- Helps you to understand new technologies as they are developed.
- Allows you to compare primary functional relationships on various network layers.

HISTORY OF OSI MODEL

Here are essential landmarks from the history of OSI model:

In the late 1970s, the ISO conducted a program to develop general standards and methods of networking.

In 1973, an Experimental Packet Switched System in the UK identified the requirement for defining the higher-level protocols.

In the year 1983, OSI model was initially intended to be a detailed specification of actual interfaces.

In 1984, the OSI architecture was formally adopted by ISO as an international standard

7 LAYERS OF THE OSI MODEL

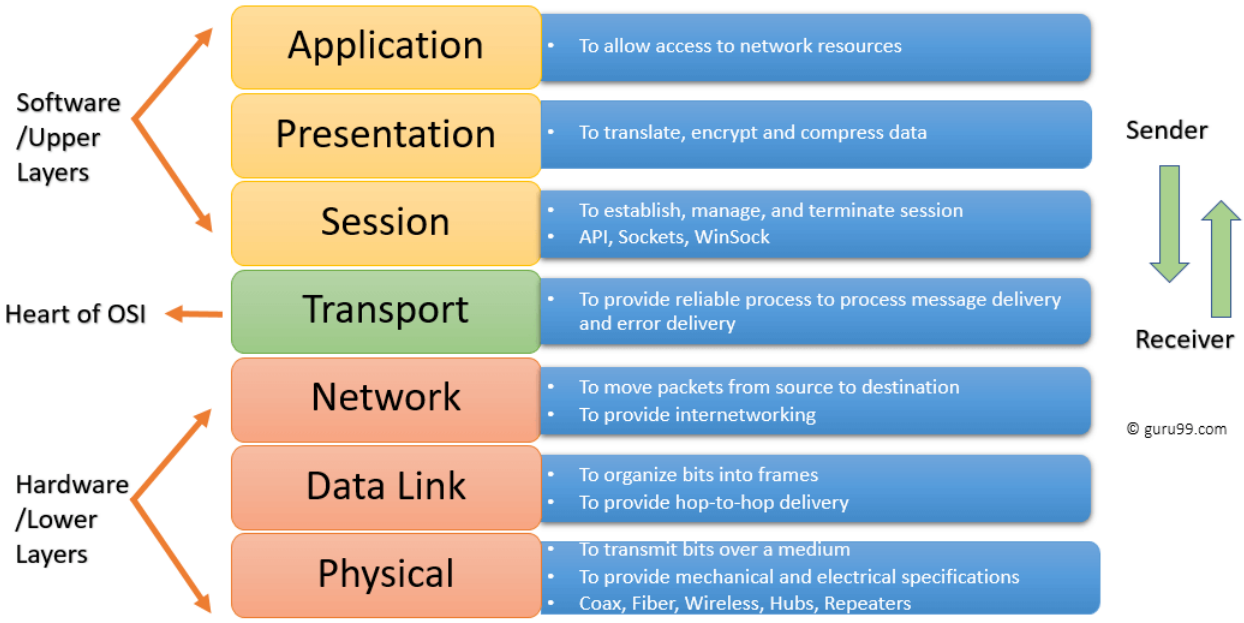
OSI model is a layered server architecture system in which each layer is defined according to a specific function to perform. All these seven layers work collaboratively to transmit the data from one layer to another.

THE UPPER LAYERS: It deals with application issues and mostly implemented only in software. The highest is closest to the end system user. In this layer, communication from one end-user to another begins by using the interaction between the application layers. It will process all the way to end-user.

THE LOWER LAYERS: These layers handle activities related to data transport. The physical layer and data link layers also implemented in software and hardware.

Upper and lower layers further divide network architecture into seven different layers as below:-

- ✓ Application
- ✓ Presentation
- ✓ Session
- ✓ Transport
- ✓ Network
- ✓ Data-link
- ✓ Physical layers



NETWORK LAYERS DIAGRAM

LET'S STUDY EACH LAYER IN DETAIL:

1. PHYSICAL LAYER

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

2. DATA LINK LAYER

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.

It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.

The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.

The data link layer is subdivided into two types of sub layers:

MEDIA ACCESS CONTROL (MAC) LAYER- It is responsible for controlling how device in a network gain access to medium and permits to transmit data.

LOGICAL LINK CONTROL LAYER- This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

IMPORTANT FUNCTIONS OF DATALINK LAYER

- ❖ Framing which divides the data from Network layer into frames.
- ❖ Allows you to add header to the frame to define the physical address of the source and the destination machine
- ❖ Adds Logical addresses of the sender and receivers
- ❖ It is also responsible for the sourcing process to the destination process delivery of the entire message.
- ❖ It also offers a system for error control in which it detects retransmits damage or lost frames.
- ❖ Data link layer also provides a mechanism to transmit data over independent networks which are linked together.

3. TRANSPORT LAYER

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the messages which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or desegmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

IMPORTANT FUNCTIONS OF TRANSPORT LAYERS

- ✓ It divides the message received from the session layer into segments and numbers them to make a sequence.
- ✓ Transport layer makes sure that the message is delivered to the correct process on the destination machine.

- ✓ It also makes sure that the entire message arrives without any error else it should be retransmitted.

4. NETWORK LAYER

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in "different networks".

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

a. Routing protocols
b. Multicast group management
c. Network-layer addresses assignment.

5. SESSION LAYER

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user's requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

IMPORTANT FUNCTION OF SESSION LAYER:

- ❖ It establishes, maintains, and ends a session.
- ❖ Session layer enables two systems to enter into a dialog
- ❖ It also allows a process to add a checkpoint to steam of data.

6. PRESENTATION LAYER

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.

This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a **SYNTAX LAYER**.

THE FUNCTION OF PRESENTATION LAYERS:

- Character code translation from ASCII to EBCDIC.
- Data compression: Allow to reduce the number of bits that needs to be transmitted on the network.
- Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
- It provides a user interface and support for services like email and file transfer.

APPLICATION LAYER

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

THE FUNCTION OF THE APPLICATION LAYERS IS:

- ✓ Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- ✓ It allows users to log on to a remote host
- ✓ This layer provides various e-mail services
- ✓ This application offers distributed database sources and access for global information about various objects and services.

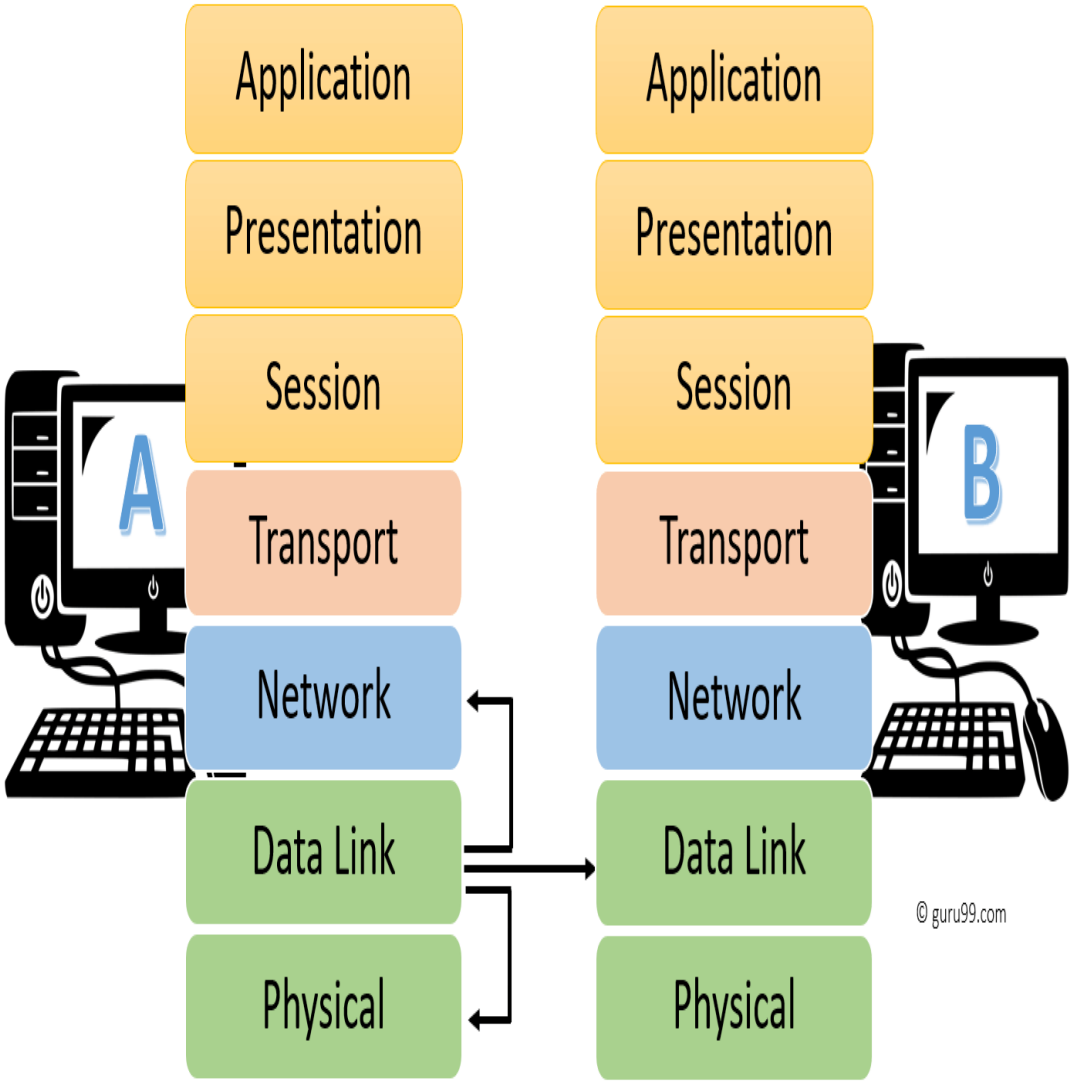
INTERACTION BETWEEN OSI MODEL LAYERS

Information sent from a one computer application to another needs to pass through each of the OSI layers.

THIS IS EXPLAINED IN THE BELOW-GIVEN EXAMPLE:

Every layer within an OSI model communicates with the other two layers which are below it and its peer layer in some another networked computing system.

In the below-given diagram, you can see that the data link layer of the first system communicates with two layers, the network layer and the physical layer of the system. It also helps you to communicate with the data link layer of, the second system.



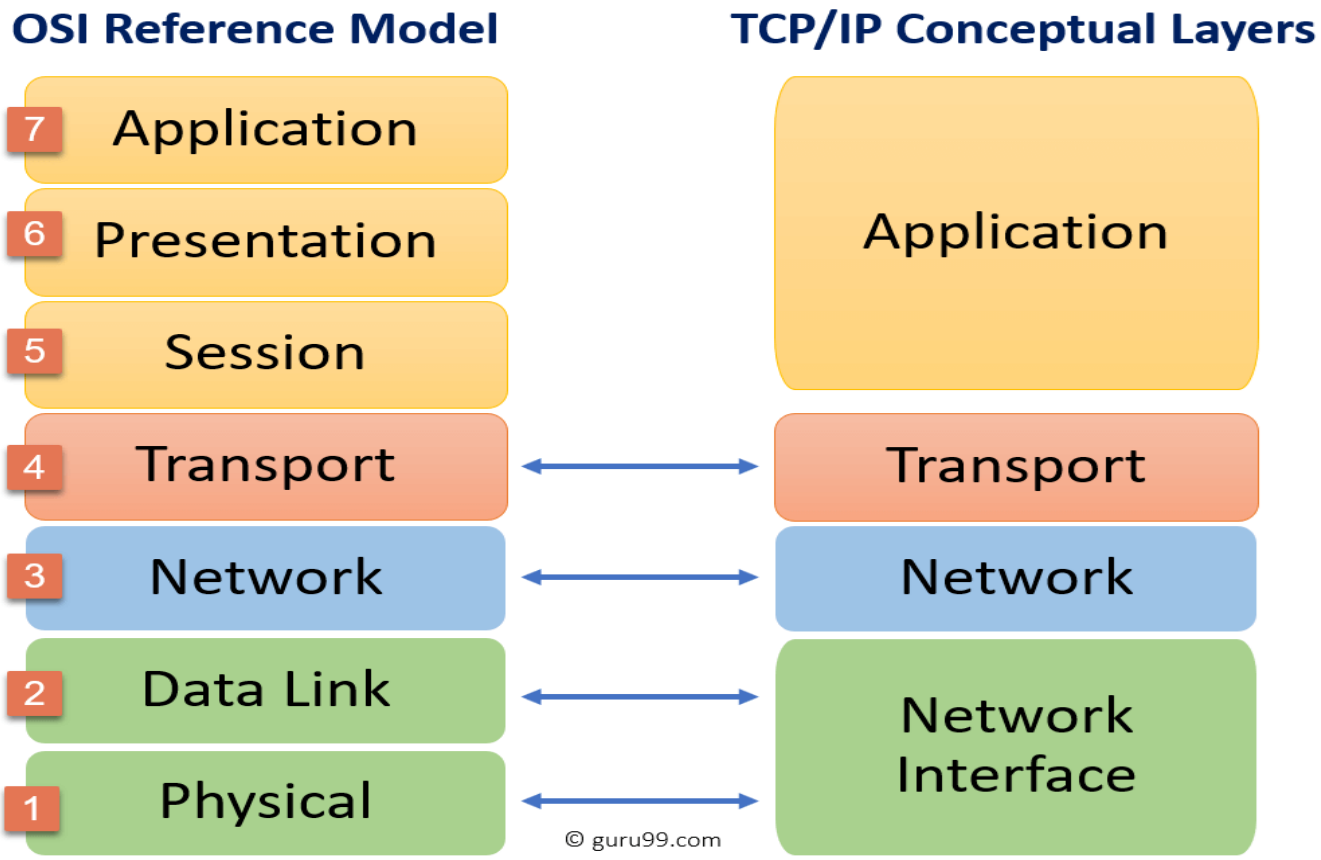
PROTOCOLS SUPPORTED AT VARIOUS LEVELS

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP

Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

DIFFERENCES BETWEEN OSI & TCP/IP

OSI MODEL	TCP/IP MODEL
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't offer any clear distinguishing points between services, interfaces, and protocols.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers	TCP/IP uses only one layer (link).
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In OSI model, data link layer and physical are separate layers.	In TCP data link layer and physical layer are combined as a single host-to-network layer.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.



ADVANTAGES OF THE OSI MODEL

Here are major benefits/pros of using the OSI model:

i. It helps you to standardize router, switch, motherboard, and other hardware
ii. Reduces complexity and standardizes interfaces
iii. Facilitates modular engineering
iv. Helps you to ensure interoperable technology
v. Helps you to accelerate the evolution
vi. Protocols can be replaced by new protocols when technology changes.
vii. Provide support for connection-oriented services as well as connectionless service.
viii. It is a standard model in computer networking.
ix. Supports connectionless and connection-oriented services.
x. Offers flexibility to adapt to various types of protocols

SUMMARY

The OSI Model is a logical and conceptual model that defines network communication which is used by systems open to interconnection and communication with other systems

In OSI model, layer should only be created where the definite levels of abstraction are needed.

OSI layer helps you to understand communication over a network

In 1984, the OSI architecture was formally adopted by ISO as an international standard.